Development of new framework for secure and efficient Voice Over IP System.

Proposal submitted for the registration of Ph.D. Degree in Computer Science.

Submitted by:

Mr. Mohamed Adan Salad Hashi

saladyare@yahoo.com

+91 9595551944

B.Sc., Hodeidah University , Hodeidah- Yemen 2013

M.Sc., Swami Ramanand Teerth Marathwada University, Nanded

Maharashtra, India 2016

Under The Guidance of

Dr. Sudhir Jagtap
(Assistant Professor)

School of computational science,

Swami Ramanand Teerth Marathwada University, Nanded

Maharashtra, India 2016.

INTRODUCTION

Voice over IP (VoIP, stands of voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques [1], VoIP is a rapid growing technology which enables the transport of voice data over Internet Protocol (IP) based networks. VoIP has become a possible alternative to Public Switched Telephone Network due to its capabilities to transport voice data in the form of digital Internet Protocol packets over the TCP/IP based Internet.

Moreover, VoIP enables users to use Internet/intranet as transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit switched Public Switched Telephone Network (PSTN) [3].

In the VoIP transmission scenario, the caller's voice is first digitized and then separated in packets using complex algorithms known as codecs. This scenario using different codecs like G.711, G.723 and G.729 for encoding and decoding the voice signal. These codecs are defined by International Telecommunication Union the Telecommunication Division (ITU-T)[2].

Today Voice over Internet Protocol (VoIP) is used in large scale to deliver voice and multimedia over the packet data networks, such as the Internet.

The Session Initiation Protocol (SIP) is widely used as a signaling protocol for VoIP. As SIP is being used more, the security of it is an important issue [4].

SIP [5] works as a signaling protocol at the application layer of the TCP/IP model. It establishes or terminates media sessions between two parties. A general SIP infrastructure consists of User Agents (UA), and several SIP servers such as registrar servers, redirect servers and SIP proxies. Here, UA and SIP proxy are more related to the scope of this paper. A UA generates, terminates, or accepts SIP requests and responses. SIP proxies forward SIP requests and responses in the SIP network.

SIP users are indicated by means of Uniform Resource Identifiers (URI), consisting of a pair of user name and domain name, (e.g.,sip:alice@abc.co.uk), which is similar to the email format.

Therefore, SIP users logically belong to different domains, and there are one or more SIP proxies in charge of processing SIP requests for each domain.

The general SIP-based telephony calling setup is shown in Figure 1. There are two SIP users in this scenario: Alice, a caller, is located in the domain abc.co.uk and Bob, a callee, is located in the domain xyz.com. First, Alice sends an INVITE request to its local proxies at (abc.co.uk). Then, the local proxies at (abc.co.uk)will forward this INVITE request to the remote proxies at (xyz.com). Then, the INVITE
request will be delivered to Bob. If Bob would like to accept the request from Alice, he will reply with a 200 OK message back through the proxies. After Alice sends an ACK message to confirm the request, the signaling handshaking is accomplished. Finally, Alice and Bob will build a media session independently without the assistant of proxies, so that they can talk in this session [6].

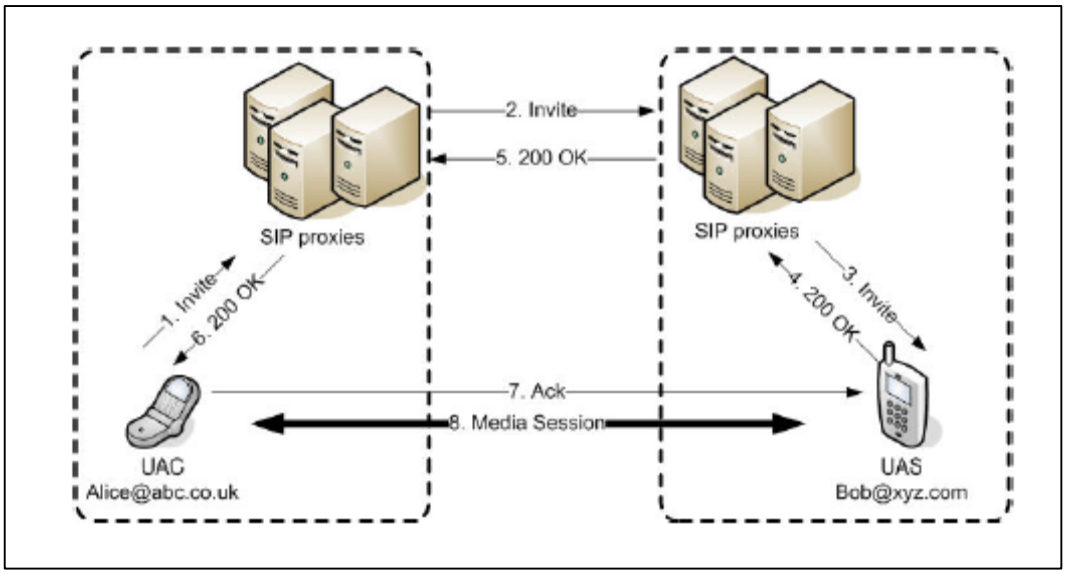

FIG1: OVERVIEW OF ESSENTIAL COMPONENTS ON SIP infrastructure

SIP is an application layer protocol developed by the IETF. Its core functionality is specified in RFC3261 [7]. Additional functionality is specified in additional RFCs [8]. SIP sessions range from ordinary calls between two participants to advanced conference sessions between multiple participants communicating over video, voice, and IM.

SIP authentication and different attacks

We shall introduce in this section SIP, authentication in general and examine two scenarios how VoIP, especially SIP, attack might be possible.

- Session Initiation Protocol (SIP)

SIP is a text-based protocol which operates at application layer [9]. It is based on request-response model, invoking some function or method with request messages and getting response as a confirm or answer to the request. SIP allows end users to negotiate stream details, for example codecs used in session, using Session Description Protocol (SDP) [10]. In SIP, registration is needed and a SIP registrar handles
that. User clients register to registrar server, which keeps record of SIP clients in that domain. As an example call flow, consider user Jack and user Joanna as in the Introduction section.

As a beginning of a SIP call, the user client of Jack initiates a call by sending an INVITE message towards Joanna. This invitation includes Jack's proposition for session description based on SDP. That INVITE message is forwarded to the client of Joanna possibly through multiple SIP proxies. After that, the client of Joanna receives the INVITE message and replies with a 180 RINGING, which is forwarded towards the client of Jack. At the time when the client of Joanna sends 180 RINGING, it also informs Joanna about the incoming SIP call, meaning basically that Joanna's SIP phone rings. If Joanna accepts the call, her client will reply to invitation with a 200 OK message, which includes Joanna's reply to the SDP received in the INVITE message.
This method of offering first a proposition of parameters and in answer receiving accepted parameters is called an offer/ answer model. When the 200 OK messages reaches back to Jack, his client will indicate Jack that the call is answered. His client can now determine the session details, accepted by the client of Joanna, from the SDP part of the received 200 OK message. Thereafter, SIP client of Jack sends an ACK message indicating the SIP phone of Joanna about the active and accepted session. From this point on, the client of Jack sends this ACK message straight to Joanna, without proxies, and the whole SIP conversation continues peer-to-peer. The addresses of the SIP user clients are learned through header fields in the messages during the exchange of the messages. The ongoing session ends, when either one sends an BYE message to the other peer.

Authentication

Authentication means identifying the object, for example person, and knowing that the identity of the object is in reality the same as the object claims it to be [11]. It is absolutely important to be sure about the identity of receiver before sending data containing for example personal information. In SIP, authentication was introduced originally through using HTTP digest mechanism, transport layer mechanism or Secure Multipart Internet Mail Extensions (S/MIME) [12]. Details of these will be explained in next section, where mechanisms for authentication in SIP are introduced.

Attack scenarios

What kind of security vulnerabilities exist? What are the threats in terms of SIP authentication? One possible threat is exposed in the registration of the user clients to the SIP registrar server, by hijacking registration of the user client. In SIP user client registration, the client sends an REGISTER message to registrar server, which includes both IP address and contact information of the user. This information can be used to hijack registration and forward incoming call to SIP phone of the hijacker. When registrar receives a request which is addressed to the user registered to the registrar receiving the request, the registrar looks for an IP address entry for the SIP contact requested. At this point hijacker might have cheated registrar by first blocking original user's registration messages by some means, for instance addressing a denial-of-service attack to user client. After blocking the user, the attacker sends its own registration messages to registrar including the SIP contact information of the original user, but with the changed IP address. In other words, the registrar thinks only the IP address of the registered user is changed and SIP contact is associated to new IP address which is the hijacker's IP address. Then registrar will forward incoming call request to the hijacker instead of the original user. [13]

In addition to register attack scenario, another type of attack is described in the article written by Cao and Jennings [14]. They introduce a threat which enables SIP calls forwarding to possibly rogue server by exploiting the lack of identifying response messages in SIP. Response identity means that responses to requests are not identified and though can be attacked. First, when SIP request is send to proxy server of the receiver, the attacker hijacks the request message and uses the header fields from that

request. Then, attacker assigns the response with status code 302, which stands for "moved temporarily" [9]. When attacker sends this response message with headers stolen from request message, for example INVITE, incoming call is forwarded to attacker.

The two attack scenarios introduced have implications on security and privacy, at least four major ones. First, attacker could get personal and confidential data of the users. Second, rogue party could mislead end users to participate to denial of service attack or third, to forward their calls to malicious voice mail. And fourth, existing call parties could be conferencing with rogue party. [14]

Authentication mechanisms in SIP

Using SIP, there exists two basic principles for providing security, end-to-end and hop-by-hop [15]. End-to-end security on SIP data involves end users, for example SIP authentication. In contrast to end-to-end solutions which use SIP mechanisms to ensure security, hop-by-hop relies on the security provided by the network. Examples of hop-by-hop mechanism are transport-level security (TLS) and Internet Protocol Security (IPsec) [15]. In terms of authentication in SIP, several mechanisms exists which we introduce in succeeding subsections. SIP specification [9] introduces HTTP digest authentication and usage of S/MIME extensions. In addition to those, we introduce also other techniques of authentication, which are designed to improve security in SIP.

HTTP digest authentication in SIP

In SIP specification [9], the authentication mechanism proposed is HTTP digest based authentication. In SIP terms, HTTP digest mechanism is called the SIP authentication. Originally, HTTP digest is a challenge-response protocol, in which a nonce value is used in challenging the target. The response includes then a checksum of the username, password, nonce value, HTTP method and requested URI. [16]

SIP applies the digest mechanism for authenticating users to users or users to proxies, not proxies to proxies. The security between proxies relies on other mechanisms, for example TLS or IPsec. First, when a server receives a request message from the client, for example INVITE, it may challenge the sender of the message. The server sends an

response message containing a nonce value and a realm towards the sender of the first request. The response is actually an error message requesting authentication. The realm in the message is the digest algorithm used in this challenge. The initiator, client, of the request receives the response and computes the response value, which is computed with nonce value received in challenge and with a username and a secret password. The secret password is known by both the client and the server. The client sends back the original request message with the computed response value, username, nonce value and realm. In figure 2 is SIP authentication mechanism as an example flow.

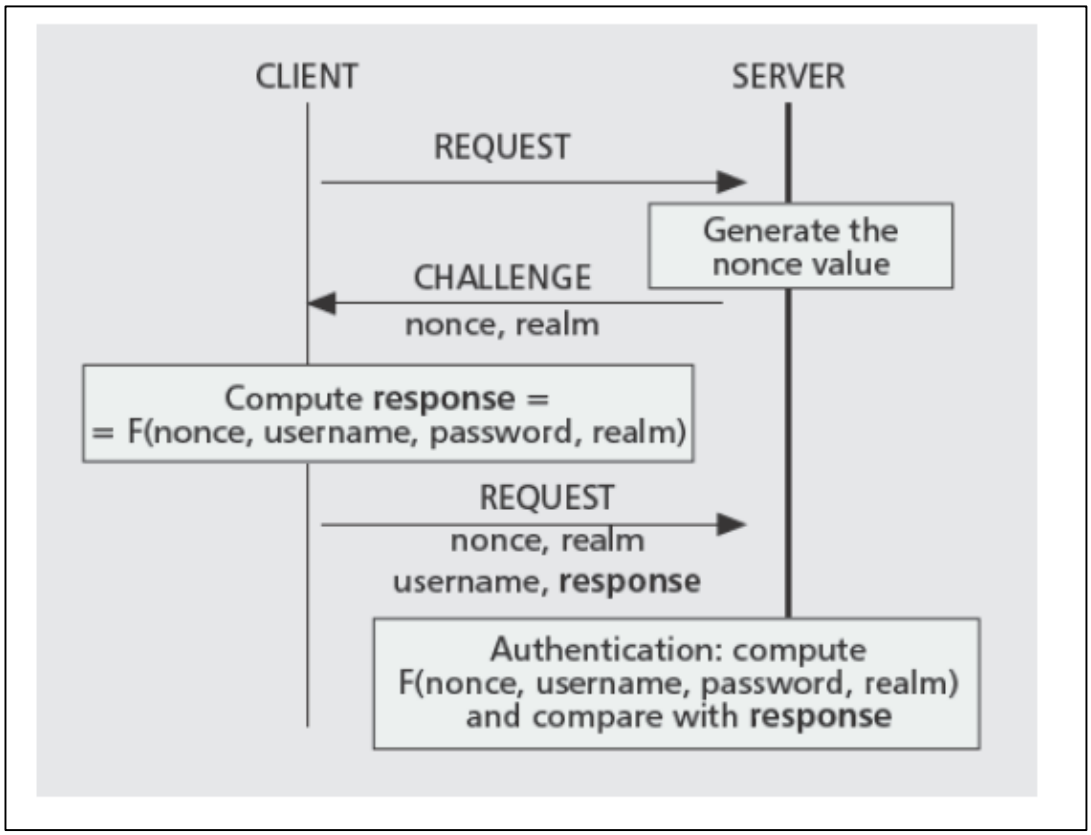

Fig.2:sip authentication based on HTTP digest

Using S/MIME in SIP for authentication

The Secure Multipart Internet Mail Extensions (S/MIME) in SIP [9] is used to carry replicates of SIP header fields inside a MIME body [14]. This enables authentication by the means of signing the replicated header fields to verify the identity of the sender. In the SIP specification [9], it is proposed to replicate all header fields inside a MIME part,

which exposes some problems. First, the SIP header fields might get altered by the intermediate SIP entities which make it difficult for the recipient to identify the legal or malicious changes in headers. Second, SIP messages can be large by their size, which causes overhead for processing and transporting of the messages. Therefore, a new solution for delivering authenticated identity of the call parties is specified by using an Authenticated Identity Body (AIB) in SIP. The AIB in SIP is a MIME body, which contains an authenticated identity. This solution of using AIB is introduced by Peterson in RFC 3893 [9].

LITERATURE SURVEY:-

The original authentication scheme for SIP-based service typically uses HTTP digest authentication protocol [18], which was found vulnerable to the off-line password guessing attacks and the server spoofing attacks [19].

Then *Yang et al.* [19] proposed an SIP authentication scheme but it is not suitable with devices with a low computational power because it works only for Discrete Logarithm (DL) setting and involves in costly exponential computation.

Unlike many legacy Time Division Multiplex (TDM) voice network that are physically separated from data-centric networks, the new VoIP networks allow the convergence of networks, Therefore , the services that that are enabled by SIP should be equally applicable to mobile and ubiquitous computing [20]. To meet this goal, based on Yang et al. scheme, *Durlanik et al.*[18] and *Wu et al*. [21] independently proposed an efficient SIP authentication scheme using Elliptic Curve Cryptosystem(ECC), which has the well-known advantages with regard to processing and size constraints [22,23] .

Mostly recently, *Yoon et al.* [20] pointed out that both *Durlanik et al.* and *Wu et al.* SIP authentication schemes are still vulnerable to off-line password guessing attacks, Denning-Sacco attacks and stolen-verifier attacks [24,25,26] and they then proposed a

new SIP authentication scheme in converge VoIP networks on ECC in order to overcome those security problem.

Qiong *Pu et al.* [27] demonstrated *Yoon et al.* scheme [20] still vulnerable to off-line password guessing attacks. There after proposed a practical SIP authentication scheme using ECC. Their scheme is quite efficient and suitable for the user's device with limited computing capability. And it is quite simple to use since it also constructs authentication with easily remembered password only.

The first pioneering work for key agreement is the Diffie-Hellman protocol given in their seminal paper [28] that invents the public key cryptography and revolutionizes the field of modern cryptography. However, the basic Diffie-Hellman protocol does not authenticate the two communication entities in the sense that an active adversary who has control over the channel can mount a man-in-the-middle attack to agree upon two separate keys with the users without the users being aware of this. This problem can be solved via a certificate which provides trusted link between the public key and the identity of the signer by the signature of Certificate Authority (CA). And there is a hierarchical framework that is called a public key infrastructure (PKI) to issue and manage certificates. However, this system requires a large amount of computing time and storage when the number of users increases rapidly.

To simplify key management procedures of conventional PKIs, *Shamir* [29] introduced the concept of Identity-Based Cryptography (IBC) in 1984, but a satisfying identity-based encryption scheme (IBE) only appeared in 2001. It was devised by *Boneh and Franklin* [30] and cleverly uses bilinear maps (the Weil or Tate pairing) over super singular elliptic curves. Subsequently, several ID-based AK protocols using pairings were proposed [31, 32].

The main practical benefit of IBC is in greatly reducing the need for, and reliance on, the public key Certificates. But IBC has the particularity to involve trusted authorities called private key generator (PKG) whose task is to compute users' private key from their identity information. The PKG can generate the secret keys of all its users, so private key escrow becomes an inherent problem in IBC. Moreover, secret keys must be sent over secure channels, which make secret key distribution a daunting task [33].

To fill the gap between traditional cryptography and identity-based cryptography, *Al-Riyami and Paterson* proposed a new paradigm called certificate less public key cryptography (CL-PKC) and the first fully-functional certificate less key agreement protocol using the Weil pairing on elliptic curves [34]. It is intended to solve the key escrow issue which is inherent in identity-based cryptography, while at the same time, eliminate the use of certificates as in the conventional Public Key Infrastructure (PKI), which is generally considered to be costly to use and manage. Due to the lack of public key authentication (certificate), it is important to assume that an adversary in the certificate less system can replace the user's public key with a false key of its choice, which is also known as key replacement attack. Cryptographic protocols including AK protocols in certificate less system are easily suffered from this kind of attack [35].

At Eurocrypt 2003, *Gentry* [33] introduced the notion of certificate-based encryption (CBE), which combines traditional pubic key encryption (PKE) with IBE while preserving most of the advantages of each. In this model, a certificate acts as a partial private key as well as a traditional public key certificate. When Bob wants to decrypt a cipher text sent from Alice, he needs both his private key and a up-to-date certificate from the CA. Hence, sender and receiver in a certificate-based public key cryptography (PKC) system are not required to obtain fresh information on certificate status each other. This approach simplifies the public key revocation problem and the certificate-based PKC does not need infrastructures like CRL [14] and OCSP [36]. In a certificate-based PKC, there is no private key escrow problem, since the CA does not know the users' private keys; and no secret key distribution problem, since the certificate need not be kept secret. But a CBE scheme is inefficient when a CA has a large number of users and performs frequent certificate updates, so Gentry suggests to use subset covers to overcome inefficiency [33]. In parallel to CBE, *Wang and CAO* [37] proposed an escrow-free certificate-based AK protocol.

Ming Luo et al. [38] gave a construction of a two-party certificate-based authenticated key agreement (CB-AK) protocol and defined a security model for the CB-AK protocol. And also show that their protocol can be used to establish keys between members of distinct domains (under different CAs) where all the CAs use different system parameters by introducing a slight modification. Furthermore, they also proved their scheme to be

secure against an uncertified user and the CA under the Bilinear Diffie-Hellman assumption and computational Diffie-Hellman assumption in the random oracle. Compared with other AK protocols regarding the robustness and computation overheads, they believed that their scheme is more efficient and more suitable for sip-based VoIP networks than previously proposed schemes.

Based on the DAA, *Undrey* [39] proposed a more flexible use of variables protected by the digest. His paper addresses the shortcomings of DAA and suggests to allow the server to decide which headers it requires to be included and protected by the digest computation. Unfortunately, his approach does not require specific headers fields to be included. Therefore, Transactions that do not include Contact fields are still vulnerable to the registration attack.

Palmieri et al. [40], [41], dismiss DAA as a usable authentication method, and instead craft a new authentication schema with digital signatures based on public-key encryption. They rely on public key infrastructure (PKI), but admit that PKI is difficult and costly to implement.

Yang et al. [42] also conclude that DAA is weak. They argue that, since DAA is vulnerable to an off-line password guessing attacks, a more secure authentication method is required. They propose an authentication method based on Diffie-Hellman. Unfortunate, they do not discuss nor add any additional SIP headers in their new authentication scheme. So their solution is also vulnerable to the registration attack.

The H.323 recommendation for the VoIP protocol from the International Telecommunication Union (ITU) has failed to see widespread adoption by industry players, and is considered abandoned in favor of SIP/RTP [43]. The authentication method in H.323, specified in H.235 [44], [45] uses well established security mechanism, like certificates, and Diffie-Hellman key exchange, to enforce authentication. Further analysis is needed to see whether the H.235 standard protects the signaling better than SIP. The Inter-Asterisk eXchange (IAX) [46], also published by the IETF, establishes a competing protocol to SIP/RTP. IAX has several security properties that are better than SIP. By multiplexing channels over the same link and transporting both signaling and media over the same port, enforcing security mechanisms is easier. IAX supports two

authentication methods: 1) MD5 Message Digest authentication [47] computed over a pre-shared secret and a challenge (nonce), or 2) using RSA public-key encryption on the challenge. In both methods, the nonce value is the only protocol parameter that is integrity protected by the authentication. Future work needs to investigate whether the IAX authentication method is adequately secure.

Other, more secure, authentication methods for SIP have been standardized, such as the support for public key encryption with S/MIME [48], the "Asserted Identity" extension [49], and the "Identity" header extension [50]. None of these authentication methods have seen any widespread deployment yet [51].

PROBLEM STATEMENT

Our aim is to the discussion of security issues of the Session Initiation Protocol (SIP), which serves as a signaling protocol for VoIP services. Especially concentrates on the security risks of SIP related to performance.And defining new secure and efficient SIP authentication scheme.

OBJECTIVES OF THE STUDY:

- To study the security issues of the Session Initiation Protocol (SIP), which serves as a signaling protocol for VoIP services?
- To present and analyze the vulnerable schemes of SIP authentication that presented in previous works.
- To improve different schemes already used for SIP authentication.
- To provide high-level security assurance to SIP VoIP service.
- To defining new secure and efficient SIP authentication scheme.
- To explore different schemes already used for SIP authentication.
- To come up with a novel scheme that optimally solves the problem.
- To validate the proposed technique using a simulation model.
- To state related factors that could be enhanced in the future.
- To give recommendations and conclusions for future enhancement.

METHODOLOGY:

- Analyzing and evaluating the different existing schemes and algorithms that are related to SIP authentication.
- Using any simulator in order to build a new technique/algorithm that could help on improving and defining schemes for SIP authentication.
- Using any simulator/tools for testing and validating the proposed schemes and technique/algorithm.

FINDINGS:-

After completing the work findings will be given.

CONCLUSION AND SUGGESTION:

After completing the work conclusion will be drawn and suggestion will be given.

PROPOSED WORK PLAN

Year-wise plan of work and targets to be achieved

Year 1:

- Literature Survey.
- Theoretical analysis of the existing different schemes already used for SIP authentication.

Year 2:

- Defining new secure and efficient scheme for SIP authentication.
- Describes an application of presented a new scheme of SIP authentication.
- Assessment of experimental results in terms of recognition rate.

Year 3:

- Interpretation of the experimental result.
- Preparation of final synopsis and thesis.
- Submission of synopsis and thesis.

REFERENCES

1. Wkipidia. Available at: http://en.wikipedia.org/wiki/Voice_over_IP.

2. S. Alshomrani, S. Qamar, S. Jan, I. Khan and I. A. Shah"QoS of VoIP over WiMAX Access Networks" in International Journal of Computer Science and Telecommunications [Volume 3, Issue 4, April 2012].

3. J. D. Gibson and B. Wei, "Tandem voice communications:Digital cellular, VoIP, and voice over wi-fi," in Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE, 2004, pp. 617-621 Vol. 2.

4. Pauli Vesterinen "User authentication in SIP" in TKK T-110.5290 Seminar on Network Security, December 2006.

5. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, 2002. RFC 3261.

6. Ge Zhang , Simone Fischer-H¨ubner , Leonardo A. Martucci , Sven Ehlert "Revealing the Calling History of SIP VoIP Systems by Timing Attacks" in International Conference on Availability, Reliability and Security, 2009.

7. SER. http://www.iptel.org, visited at 16th-Sep-2008.

8. "IETF Session Initiation Protocol Core Charter." [Online]. Available: http://datatracker.ietf.org/wg/sipcore/charter/ [Accessed: 1. Nov 2011].

9. Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M. and Schooler E. SIP: Session Initiation Protocol. RFC 3261, IETF Network Working Group, June 2002.

10. Handley J. and Jacobson V. SDP: Session Description Protocol. RFC 2327, IETF Network Working Group, April 1998.

11. Lowe Gavin. A Hierarchy of Authentication Specifications.Computer Security Foundations Workshop, 1997. Proceedings, June 1997. Page(s): 31-43.

12. Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M. and Schooler E. SIP: Session Initiation Protocol. RFC 3261, IETF Network Working Group, June 2002.

13. Thermos Peter. Two attacks against VoIP. SecurityFocus, April 2006.

14. Cao F. and Jennings C. Providing response identity and authentication in IP telephony. Availability, Reliability and Security, April 2006.

15. Salsano Stefano, Veltri Luca and Papalilo Donald ." SIP security issues: the SIP authentication procedure and its processing load". *IEEE Network*, Volume 16, Issue 6, Nov-Dec 2002. Page(s): 38-44.

16. Franks J., Hallam-Baker P., Hostetler J., Lawrence S., Leach P., Luotonen A. and Stewart L. HTTP Authentication: Basic and Digest Access Authentication. RFC 2617, IETF Network Working Group, June 1999.

17. Peterson J. Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format. RFC 3893, IETF Network Working Group, September 2004.

18. Franks J. ,Hallam-Baker P.,Hostetler J. , Lawrence S., Leach P. , Luotonen A., and Stewart L.,"HTTP Authentication : Basic and Digest Access Authentication", Technical Document Internet Engineering Task Force RFC,1999.

19. Yang C. Wang R.,and Liu W.,"Secure Authentication Scheme for Session Initiation Protocol" Computer and security ,Vol.24 ,no.5,pp. 381-386,2005.

20. Yoon E., Yoo K., Kim C.,Hong Y., Jo M., and Chen H.,"A Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks." Computer Communications, vol. 33 ,no. 14,pp.1674-1681,2010.

21. Wu L., Wang F. , and Zhang Y.,"An Efficient User Authentication and Key Exchange Protocol for Mobile Client-Server Environment," Computer Networks ,vol.54,no. 9,pp. 1520-1530,2009.

22. Hankerson D.,Menezes A., and Vanstone S.,Guide to Elliptic Curve Cryptography, Springer-Verlag,USA,2004.

23. Koblitz N., " Elliptic Curve Cryptosystem," Mathematics of Computation,Vol. 48,no. 177,pp. 203-209,1987.

24. Denning D. and Sscco G.,"Timestamps in Key Distribution Systems," Communications of The ACM, vol. 24, no. 8,pp. 533-536.

25. Menezes A., Oorschot P., and Vanstone S., Handbook of Applied Cryptograph, CRC press, New York, 1997.

26. Lin C. and Hwang T., "A Password Authentication Scheme with Secure Password updating," Computers and Security ,Vol. 22, no. 1, pp. 68-72,2003.

27. Qiong Pu and Shuhua Wu , " Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks." In The International Arab Journal of information Technology ,Vol. 9,no. 6,pp. 553-561, November 2012.

28. W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, pp. 644 – 654, 1976.

29. A. Shamir. Identity-based cryptosystems and signature schemes. Advances in Cryptology - CRYPTO'84. LNCS 196, pp. 47–53, 1984.

30. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. Proc. of the Crypto 2001. LNCS 2139, pp. 213-229, 2001.

31. E. Ryu, E. Yoon and K. Yoo. An efficient ID-based authenticated key agreement protocol from pairings. Proc. NETWORKING'04. LNCS 3042, pp. 1458-1463, 2004.

32. N. McCullagh and P. S. L. M. Barreto. A New Two-Party Identity-Based Authenticated Key Agreement. Cryptology ePrint Archive, Available online: http://eprint.iacr.org/2004/122.

33. C. Gentry. Certificate-based Encryption and the Certificate Revocation Problem. Advances in Cryptology-EUROCRPYT 2003, LNCS 2656, pp. 272–293, 2003.

34. S.S. Al-Riyami, K.G. Paterson. Certificateless Public Key Cryptography. Advances in Cryptography-ASIACRYPT 2003, LNCS 2894, pp.452–473, 2003.

35. B.C. Hu, D.S. Wong and Z.F. Zhang. Key Replacement Attack against a Generic Construction of Certificateless Signature. Proc. ACISP 2006, LNCS 4058, pp. 235–246, 2006.

36. M. Myers, R. Ankney and A. Malpani. X.509 internet public key infrastructure online certificate status protocol – OCSP. RFC 2560, 1999.

37. S.B. Wang Z.F. CAO. Escrow-Free Certificate-Based Authenticated Key Agreement Protocol from Pairings. Wuhan University Journal of Natural Sciences, vol 12, pp. 63-66, 2007.
38. Ming Luo, Ying-You Wen and Hong Zhao, "A Certificate-Based Authenticated Key Agreement Protocol for SIP-Based VoIP Networks" in IFIP International Conference on Network and Parallel Computing.

39. J. Undery, "Ieft draft: SIP authentication: SIP digest access authentication," IETF, Tech. Rep., Jul. 2001.

40. F. Palmieri, "Improving authentication in voice over IP infrastructures," in Advances in Computer, Information, and Systems Sciences, and Engineering, K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, Eds. Springer Netherlands, 2006, pp. 289 – 296. [Online]. Available: http://www.springerlink.com/content/pj11582775h177q0/ Accessed: 1. Nov 2011].

41. F. Palmieri and U. Fiore, "Providing true end-to-end security in converged voice over IP infrastructures," Computers & Security, vol. 28, no. 6, pp. 433–449, Sep. 2009.

42. C. Yang, R. Wang, and W. Liu, "Secure authentication scheme for session initiation protocol," Computers & Security, vol. 24, no. 5, pp. 381–386, Aug. 2005.

43. H. Sinnreich and A. B. Johnston, Internet communications using SIP: Delivering VoIP and multimedia services with Session Initiation Protocol, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., August 2006.

44. International Telecommunication Union, "H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems," ITU-T Recommendation H.235.0, 2005.

45. ——, "H.323 security: Framework for secure authentication in RAS using weak shared secrets," ITU-T Recommendation H.235.5, 2005.

46. M. Spencer, B. Capouch, E. Guy, F. Miller, and K. Shumard, "IAX: Inter-Asterisk eXchange Version 2," RFC 5456 (Informational), Internet Engineering Task Force, Feb. 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5456.txt Accessed: 1. Nov 2011].

47. R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321 (Informational), Internet Engineering Task Force, Apr. 1992. [Online]. Available: http://www.ietf.org/rfc/rfc1321.txt [Accessed: 1. Nov 2011].

48. J. Peterson, "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)," RFC 3853 (Proposed Standard), Internet Engineering Task Force, Jul. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3853.txt [Accessed: 1. Nov 2011].

49. C. Jennings, J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," RFC 3325 (Informational), Internet Engineering Task Force, Nov. 2002, updated by RFC 5876. [Online]. Available: http://www.ietf.org/rfc/rfc3325.txt [Accessed: 1. Nov 2011].

50. J. Peterson and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," RFC 4474 (Proposed Standard), Internet Engineering Task Force, Aug. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4474.txt [Accessed: 1.Nov 2011].

51. D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Schulzrinne, SIP Security. WileyBlackwell, Mar. 2009.

Researcher

Mohamed Adan Salad Hashi

Guide

Dr. Sudhir Jagtap